Sabita J. Soneji, California Bar No. 224262
ssoneji@tzlegal.com
TYCKO & ZAVAREEI LLP
1970 Broadway
Suite 1070
Oakland, CA 94612
Telephone: (510) 254-6808

[Additional Counsel Listed on Signature Page]

Attorneys for Plaintiffs and the Proposed Classe

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

VALERIE LOZOYA, JOLINDA MURPHY, LAUREN NEVE, AND MOLLY O'HARA, *on behalf of themselves and all others who are similarly situated*,

Plaintiffs,

v.

TICKETMASTER LLC, and LIVE NATION ENTERTAINMENT, INC.,

Defendants.

Case No. 8:25-cv-00202

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Eric Anderson, Tiffany Moore, and Dekima Thomas bring this Class Action Complaint, both individually and on behalf of all others similarly situated, against Defendants Live Nation Entertainment, Inc., and Ticketmaster LLC (collectively, "Ticketmaster"). Plaintiffs' allegations are based on personal knowledge and belief and the investigation of counsel.

INTRODUCTION

1. Data companies are acutely aware of the critical importance of cybersecurity in an increasingly interconnected world. With the exponential growth of cloud storage, companies are entrusted with sensitive information, ranging from personal details to financial records.

2. Defendants Ticketmaster, LLC and Live Nation Entertainment, Inc. (together "Defendants") did not keep the personal information they collected from class members secure.

3. Defendants have long understood the importance of robust cybersecurity to protect consumer data. Information security policies and practices are imperative to ensuring that sensitive information is not exposed to unauthorized third parties. These exposures, commonly referred to as "data breaches," can cause significant harm to individuals—exposing them to fraud and attempted fraud, identity theft, reputational harm, and the continuing risk of harm that results from criminals having their sensitive information.

4. A single data breach can result in catastrophic consequences for individuals. As a result, and based upon legal and industry-standard requirements, companies prioritize robust cybersecurity measures.

5. In this case, however, none of the Defendants implemented three of the most basic and industry-standard cybersecurity policies to protect Personal Information, including most prominently, multifactor authentication (MFA).[1] The

[1] "Personal Information," as used herein, refers to that information which was exposed

foreseeable result: a data breach.

6. Defendants use a cloud storage company called Snowflake to keep the Personal Information they collected secure. But that information was not secure. The cybercriminal known as UNC5537 used compromised login credentials for Defendants, plugged them in to Defendants' Snowflake accounts, and successfully exfiltrated Personal Information relating to hundreds of millions of consumers.

7. UNC5537's success was made possible by basic data security failings on the part of Defendants. These companies collectively flouted relevant governmental guidance, regulations, statutes, and industry standards.

8. The Data Breach's foreseeable consequences are neither imaginary nor hypothetical: shortly after the Data Breach, sensitive information previously stored with Snowflake began appearing for sale on the Dark Web.[2] The harm resulting from allowing this information to be exposed cannot be undone.

9. Plaintiffs and Class Members[3] now face the real and actual harm that the Data Breach has caused them and will continue to cause them. Not only have cybercriminals obtained valuable and sensitive Personal Information about them, but that information has been obtained by other criminals, and offered for resale to still more criminals. As a result, Plaintiffs and Class Members have already experienced fraud or potential fraud, an invasion of their privacy, time and expenses spent mitigating the imminent and substantial risk of data misuse, and are at significant risk of identity

---

to cybercriminals through the Data Breach. While the information exposed varies from each Defendant, each protected that information behind credentials (i.e., a username and password), intending that it not be exposed to unauthorized third parties. As alleged herein, inadequate, negligent, and reckless cybersecurity practices resulted in that information being exposed.

[2] Snowflake Breach Threat Actor Offers Data of Cloud Company's Customers, SOCRadar, https://socradar.io/overview-of-the-snowflake-breach/ (last accessed Jan. 13, 2024).

[3] "Class Members" refers to those individuals who were impacted by the Data Breach, as alleged herein. Specific class definitions for each Defendant are provided in the relevant sections.

theft, reputational harm, and other injuries.

10. Defendants bears responsibility for their role in the Data Breach. Despite their experience and sophistication, Defendants were negligent (at best) and reckless (at worst) for failing to implement basic and routinely required cybersecurity practices to protect Plaintiffs' and Class Members' Personal Information.

PARTIES

I. Defendants

11. **Live Nation Entertainment, Inc.** is an entertainment company incorporated under Delaware law, with its principal place of business located at 9348 Civic Center Drive, Beverly Hills, California.[4]

12. **Ticketmaster, LLC** is a ticket distribution company for entertainment events, and is a wholly owned subsidiary of Live Nation.[5] Ticketmaster is a Virginia limited liability company, with its principal place of business located at 9348 Civic Center Drive, Beverly Hills, California.[6]

II. Plaintiffs

13. **Plaintiff Valerie Lozoya** is a citizen of California residing in Hawthorne. Plaintiff Lozoya received a data breach notice letter, via U.S. mail, directly from Ticketmaster, dated July 17, 2024. Plaintiff Lozoya is a current customer of Ticketmaster and has regularly purchased tickets. In doing so, she provided Ticketmaster with at least her name, address, email, phone number, and payment card information.

14. As a result of the Data Breach, Plaintiff Lozoya has suffered injury and

---

[4] Live Nation Entertainment, Inc., Annual Report (Form 10-K) (Feb. 22, 2024) ("LiveNation 2024 10-K"), https://www.sec.gov/Archives/edgar/data/1335258/000133525824000017/lyv-20231231.htm.

[5] LiveNation 2024 10-K at 54.

[6] Ticketmaster, LLC, *Statement of Information*, Cal. Sec'y of State (Sept. 25, 2024), https://bizfileonline.sos.ca.gov/api/report/GetImageByNum/253133124121113249074045085047228112143236158047.

damages, including but not limited to, the unauthorized use of her stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent obtaining credit monitoring services and reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of her Personal Information; invasion of her privacy; and emotional distress and anxiety resulting from the theft of her Personal Information and responding to identity theft.

15. **Plaintiff Jolinda Murphy** is a citizen of Montana residing in Missoula. Plaintiff Murphy received a data breach notice letter, via U.S. mail, directly from Ticketmaster, dated July 17, 2024. Plaintiff Murphy is a customer of Ticketmaster, but she cannot recall the last time she purchased tickets. She does recall that, when she did purchase tickets, she provided Ticketmaster with at least her name, address, email, phone number, and payment card information.

16. As a result of the Data Breach, Plaintiff Murphy has suffered injury and damages, including but not limited to, the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent obtaining credit monitoring services and reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of her Personal Information; invasion of her privacy; and emotional distress and anxiety resulting from the theft of her Personal Information.

17. **Plaintiff Lauren Neve** is a citizen of California residing in San Juan Capistrano. Plaintiff Neve is a former customer of Ticketmaster, where she last purchased a ticket in 2022 and in doing so, provided Ticketmaster with at least her name, address, email, and payment card information.

18. As a result of the Data Breach, Plaintiff Neve has suffered injury and damages, including but not limited to, the unauthorized use of her stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent obtaining credit

monitoring services and reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of her Personal Information; invasion of her privacy; and emotional distress and anxiety resulting from the theft of her Personal Information and responding to identity theft.

19. **Plaintiff Molly O'Hara** is a citizen of Massachusetts residing in Revere. Plaintiff O'Hara received a data breach notice letter, via U.S. mail, directly from Ticketmaster, dated July 9, 2024. Plaintiff O'Hara is a current customer of Ticketmaster who has regularly purchased tickets. In doing so, she provided Ticketmaster with at least her name, address, email, phone number, and payment card information.

20. As a result of the Data Breach, Plaintiff O'Hara has suffered injury and damages, including but not limited to, the unauthorized use of her stolen Personal Information; the substantial risk of identity theft and reasonable mitigation efforts spent to protect against such risks, including time and expenses spent obtaining credit monitoring services and reviewing financial accounts for fraudulent activity; loss of property and value of that property with respect to the inability to control use of her Personal Information; invasion of her privacy; and emotional distress and anxiety resulting from the theft of her Personal Information and responding to identity theft.

JURISDICTION AND VENUE

21. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, and Defendants are citizens of States different from that of at least one Class member. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

22. Venue is proper in this Court because Defendants are domiciled in this State, and have conducted business in this State. The Court has personal jurisdiction over the Defendants because they are all headquartered in this State.

FACTUAL ALLEGATIONS

23. Consumers are largely unable to purchase concert tickets or enjoy concerts without working through Live Nation, and its wholly owned subsidiary, Ticketmaster.

24. Live Nation and Ticketmaster control approximately 70% of the American market for live event ticketing, selling hundreds of millions of tickets per year.[7] Live Nation reported a quarterly revenue of $7.7 billion in November 2024.[8]

25. Ticketmaster requires consumers who purchase tickets on their platform to provide their Personal Information to Ticketmaster, both to facilitate the ticket sales and for Ticketmaster's own business purposes. Ticketmaster promises to keep consumers' Personal Information secure and does not allow consumers to opt out of sharing their Personal Information.

26. Ticketmaster made express commitments to protect consumer Personal Information in its Privacy Policy, assuring consumers in a caption titled, Looking After Your Information, "We have security measures in place to protect your information."[9]

27. Ticketmaster publicly represented that data security forms a crucial aspect of its business model. For instance, on a segment of Ticketmaster LLC's website, the company stated:

"Our goal is to maintain your trust and confidence by handling your personal information with respect and putting you in control."[10]

---

[7] Daniel Allen, *Does Live Nation Own Ticketmaster? The Complete Story Behind Entertainment's Biggest Merger, The Ticket Lover* (Oct. 28, 2024), https://theticketlover.com/does-live-nation-own-ticketmaster/).

[8] Live Nation, *LIVE NATION ENTERTAINMENT REPORTS THIRD QUARTER 2024 RESULTS* (Nov. 11, 2024), https://www.livenationentertainment.com/2024/11/live-nation-entertainment-reports-third-quarter-2024-results/.

[9] Ticketmaster, *PRIVACY POLICY: Looking After Your Information*, https://web.archive.org/web/20240226040956/https://privacy.ticketmaster.com/privacy-policy#looking-after-your-information (archived Feb. 26, 2024).

[10] Ticketmaster, *PRIVACY POLICY: Our Commitment To You*, https://web.archive.org/web/20240226040956/https://privacy.ticketmaster.com/pri

"As a global company, our fans are located all over the world, depending on your market there are specific laws and regulations around privacy rights such as the GDPR in Europe, LGPD in Brazil and CCPA in United States."[11]

"We have security measures in place to protect your information."[12]

28. Live Nation also maintained a privacy policy section, affirming its adherence to various state and federal laws.[13]

29. Defendants are Snowflake customers. Ticketmaster stores the Personal Information of its consumers on Snowflake's Data Cloud services, which include customers' names, addresses, contact information (email and phone numbers), and payment card information.

30. In 2024, Defendants had a data breach involving personal information stored in Snowflake's cloud (the "Data Breach").

31. The events leading up to the Data Breach and its fallout are summarized in a June 10, 2024 report published by Mandiant (the "Mandiant Report"), a cybersecurity firm that assisted Snowflake in its investigation of the Data Breach.[14]

32. The Data Breach occurred because Defendants did not follow basic, routinely-adopted, best-practice, necessary, and standard cybersecurity guidelines.

---

vacy-policy#our-commitment-to-you (archived Feb. 26, 2024).

[11] Ticketmaster, *PRIVACY POLICY: Your Choices & Rights*, https://web.archive.org/web/20240226040956/https://privacy.ticketmaster.com/privacy-policy#your-choices-&-rights (archived Feb. 26, 2024).

[12] *Id.*

[13] Live Nation, *PRIVACY POLICY: Looking After Your Information*, https://web.archive.org/web/20240226040956/https://privacy.ticketmaster.com/privacy-policy#looking-after-your-information (archived Feb. 26, 2024).

[14] Mandiant, *UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion*, Google Cloud (June 10, 2024), https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion ("*Mandiant Report*"). Since Snowflake had a hand in the Mandiant Report, the events are likely worse than presented, and will be clarified in discovery. *See also Snowflake Breach: Hacker Confirms Access Through Infostealer Infection*, Hudson Rock, https://archive.is/tljkW (archived website).

33. According to the Mandiant Report, the success of UNC5537's straightforward cyberattack was made possible by "three primary factors" on the part of Defendants.

34. **First**, Defendants did not have MFA enabled. MFA is a basic and industry-standard cybersecurity measure, available for nearly three decades,[15] that requires a user to, in addition to providing their username and password, further authenticate their identity through another source, such as through a passcode sent by text message or email.[16] Without MFA, a valid username and password was all UNC5537 needed to access a Snowflake customer's data—similar to a key placed under a doormat.

35. **Second**, Defendants did not have policies and procedures in place to rotate or disable stale credentials.

36. **Third**, Defendants did not restrict access to Snowflake cloud-based storage based upon certain trusted locations. Conditional Access Policies allow companies to fine-tune access to control from which devices and locations users can access resources. Again, without such protection, a valid username and password entered was all UNC5537 needed to access Defendants' data from anywhere at any time.

37. As set out in more detail herein, Plaintiffs' and Class Members' Personal Information have already been sold and exchanged on the dark web between UNC5537 and various other cybercriminal threat actors.

---

[15] Bojan Šimić, *Identity in the Digital Age and the Rise of Multi-Factor Verification*, Forbes (Oct. 10, 2024), https://www.forbes.com/councils/forbestechcouncil/2024/10/10/identity-in-the-digital-age-and-the-rise-of-multi-factor-verification/ (MFA was developed by AT&T as a system to exchange codes on two-way pagers).

[16] Rose de Fremery, *Tracing the Evolution of Multi-Factor Authentication*, LastPass (Oct. 16, 2023), https://blog.lastpass.com/posts/tracing-the-evolution-of-multi-factor-authentication.

I. The Data Breach harmed Plaintiffs and Class Members.

38. The effects of the Data Breach were felt immediately—not only by Defendants—but by individual consumers. Personal Information is valuable property. Its value is axiomatic, considering the market value and profitability of "Big Data" to corporations in America.

39. Information protected by credentials—usernames and passwords—is intended to stay private, and not disclosed to third parties (otherwise, why password-protect the information, at all?). But because of Defendants' failure to follow basic cybersecurity guidelines, the information stored on Snowflake's cloud-based servers was accessible to cybercriminals, who exfiltrated the data for nefarious purposes.

40. Ticketmaster's failings were particularly egregious given the enormous amount of Personal Information it stored on Snowflake's servers. Tasked with handling the data of over 560 million consumers, Ticketmaster's failure to implement basic data security measures is all the more inexplicable and reckless.

41. Defendants have disclosed that certain types of Personal Information were exposed in the Data Breach. To date, Defendants have confirmed at least the following consumer data was exposed: consumer name, contact information, last four digits of credit card numbers and expiration dates, ticket order details.[17]

42. The Personal Information exposed is extremely valuable and can be used for a number of nefarious purposes.

43. Information from this Data Breach has already been found in several places on the dark web—even reappearing after law enforcement agencies shut down certain websites offering information for sale.[18]

---

[17] Ticketmaster, Notice of Data Breach (July 8, 2024) ("Ticketmaster Notice"), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/0d26b6dd-b466-4f2a-bec0-ec2ad0738583.html.

[18] *See, e.g.*, Ionut Arghire, *Hackers Boast Ticketmaster Breach on Relaunched BreachForums*, SecurityWeek (May 31, 2024), https://www.securityweek.com/hackers-boast-

44. Identity thieves use Personal Information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[19] According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to, among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; or use the victim's information in the event of arrest or court action.[20]

45. Exposed driver's license numbers are sold on the dark web for as much as $20 a piece because they can be used to create counterfeit licenses, open financial accounts, cash counterfeit checks, and even obtain medical care using someone's

---

ticketmaster-breach-on-relaunched-breachforums/; Sergiu Gatlan, *Advance Auto Parts stolen data for sale after Snowflake attack*, Bleeping Computer (June 5, 2024), https://www.bleepingcomputer.com/news/security/advance-auto-parts-stolen-data-for-sale-after-snowflake-attack/; Jessica Lyons, *Fiend touts stolen Neiman Marcus customer infor for $150k*, The Register (June 25, 2024), https://www.theregister.com/2024/06/25/neiman_marcus_snowflake_victim/.

[19] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things: "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id.*

[20] See Louis DeNicola, *What Can Identity Thieves Do with Your Private Information and How Can You Protect Yourself*, Experian (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

identity.[21] Exposed gift cards can result in their balances being reduced to nothing.[22] Individuals may also experience theft of their event tickets.[23]

46. Each additional piece of Personal Information exposed in a data breach increases an individual's risk of identity fraud and exposure to scams. Information from one breach may be combined with information from other breaches to create "fullz"—or complete information about an individual sufficient to facilitate identity theft, allow for the purchase of goods and services on the internet, and enable criminals to open new accounts in a victim's name.[24]

47. The exposure of Personal Information in the Data Breach has subjected the Plaintiffs to actual and imminent harm that is concrete and particularized.

48. Defendants did not take sufficient steps to protect their customers, and have not done nearly enough to compensate the victims of the Data Breach, who will

---

[21] *How driver's licenses exposed in data breaches increase your risk of identity fraud*, IDX (May 6, 2021), https://www.idx.us/knowledge-center/how-drivers-licenses-exposed-in-data-breaches-increase-your-risk-of-identity-fraud; John Egan, *What Should I Do if My Driver's License Number Is Stolen*, Experian (June 13, 2024), https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/.

[22] Jackie Callaway, *Beware: Hackers can steal money off gift cards before you have a chance to use them*, ABC News Tampa Bay (Dec. 29, 2020), https://www.abcactionnews.com/money/consumer/taking-action-for-you/beware-hackers-can-steal-money-off-gift-cards-before-you-have-a-chance-to-use-them.

[23] Taylor O'Bier, *Hackers allegedly leak tickets from Ticketmaster to Talyor Swift tour and more*, Scripps (Jul. 10, 2024), https://www.scrippsnews.com/science-and-tech/data-privacy-and-cybersecurity/hackers-allegedly-leak-tickets-from-ticketmaster-to-taylor-swift-tour-and-more ("Sp1d3rHunters hit back, stating in another forum post that the ticket information they allegedly stole was for physical ticket types and therefore they can't be refreshed. If this is true, Ticketmaster would have to void and reissue all the stolen tickets.").

[24] Robert Lemos, *All about your 'fullz' and how hackers turn your personal data into dollars*, PCWorld (June 2, 2016), https://www.pcworld.com/article/414992/all-about-your-fullz-and-how-hackers-turn-your-personal-data-into-dollars.html; Paige Tester, *What are Fullz? How Hackers & Fraudsters Obtain & Use Fullz*, DataDome (Mar. 3, 2023), https://datadome.co/guides/account-takeover/what-are-fullz-how-do-fullz-work/.

suffer real harm for years to come.

CLASS ACTION ALLEGATIONS

49. Plaintiffs bring this action on their own behalf, and on behalf of the following Class:

All individuals residing in the United States whose Personal Information was compromised in the Data Breach.

50. Excluded from the Class are Defendants' officers and directors, any entity in which a Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

51. Plaintiffs reserve the right to amend or modify the definition of the Class or create additional subclasses as this case progresses.

52. **Numerosity.** The members of the Ticketmaster Classes are so numerous that joinder of all of them is impracticable.

53. **Commonality.** There are questions of fact and law common to the Ticketmaster Classes, which predominate over individualized questions. These common questions of law and fact include, but are not limited to:

a. Whether Ticketmaster and Live Nation had a duty to protect the Personal Information of Ticketmaster Plaintiffs and Class Members.

b. Whether Ticketmaster and Live Nation breached express or implied commitments to protect the Personal Information of Ticketmaster Plaintiffs and Class Members.

c. Whether Ticketmaster and Live Nation knew or should have known that their data security practices were deficient.

d. Whether Ticketmaster and Live Nation's data security systems were consistent with industry standards prior to the Data Breach.

e. Whether Ticketmaster and Live Nation adequately disclosed details regarding the Data Breach to affected consumers.

f. Whether Ticketmaster unlawfully utilized, retained, misplaced, or exposed Plaintiffs' and the Class Members' Personal Information.

g. Whether Ticketmaster Plaintiffs and Class Members are entitled to actual damages, punitive damages, treble damages, statutory damages, general damages, nominal damages, and/or injunctive relief.

54. **Typicality.** Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Personal Information, like that of every other Class Member, was compromised in the Data Breach.

55. **Adequacy of Representation.** Plaintiffs will fairly and adequately represent and protect the interest of the Class Members. Plaintiffs' Counsel are competent and experienced in litigating class actions.

56. **Predominance.** Defendants have engaged in a common course of conduct toward Plaintiffs and the Class Members, in that all the data of Plaintiffs and Class Members were stored on the same Snowflake Data Cloud network and unlawfully accessed in the same manner. The common issues arising from Defendants' conduct affecting Class Members listed above predominate over any individualized issues. Adjudication of these common issues in a single action will advance judicial economy.

57. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the claims of the Class. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation.

58. **Injunctive Relief.** Defendants have acted on grounds that apply generally to the Class as a whole such that class certification, injunctive relief, and declaratory relief are appropriate on a class wide basis.

59. **Issue Certification.** Likewise, particular issues are appropriate for

certification because such claims present common issues whose resolution would advance the disposition of this matter.

60. **Identification of Class Members Using Objective Criteria.** Finally, all members of the proposed Ticketmaster Classes are readily identifiable using objective criteria. Defendants have access to the names and contact information of Class Members affected by the Data Breach.

CAUSES OF ACTION

FIRST CLAIM FOR RELIEF
Negligence
On Behalf of Plaintiffs and the Class

61. Plaintiffs repeat and re-allege the allegations above as if fully set forth herein.

62. Defendants owed a duty under common law to the Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, and deleting their Personal Information in its possession from being compromised, stolen, or misused by unauthorized persons.

63. Specifically, this duty included, among other things: (a) implementing industry standard data security safeguards to protect the Personal Information of Plaintiffs and the Class Members such as MFA, rotating credentials, and restricting access privileges; (b) maintaining, testing, and monitoring Defendants" security systems to ensure that Personal Information was adequately secured and protected; (c) timely acting upon warnings and alerts to respond to intrusions; and (d) adequately notifying the Plaintiffs and Class Members about the types of data that were compromised in the Data Breach.

64. Defendants' duty to use reasonable care arose from several sources, including that Defendants knew the information they were storing was private and sensitive, and that failing to take adequate steps to secure and protect the data would foreseeably lead to a Data Breach which could injure individual consumers.

65. Defendants had a common law duty to prevent foreseeable harm to

others. This duty existed because Defendants collected and stored valuable Personal Information that is routinely targeted by cyber criminals. Plaintiffs and Class Members were the foreseeable and probably victims of any compromise to inadequate data security practices maintained by Defendants.

66. Defendants breached their duties owed to Plaintiffs and Class Members by failing to maintain adequate data security practices that conformed with industry standards, and were therefore negligent.

67. Defendants breached their duties owed to Plaintiffs and Class Members by failing to exercise reasonable oversight in the selection of Snowflake to store Personal Information. Such reasonable oversight would have revealed that Snowflake's cloud services lacked industry standard data security safeguards necessary to adequately protect Personal Information.

68. But for Defendants' negligence, the Personal Information of Plaintiffs and Class Members would not have been stolen by cybercriminals in the Data Breach.

69. As a direct and proximate result of Defendants' breach of duties, Plaintiffs and Class Members have suffered injuries as detailed herein.

70. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members are entitled to damages, including compensatory, general, nominal. and/or punitive damages, in an amount to be proven at trial.

SECOND CLAIM FOR RELIEF
Violation of Applicable State Consumer Protection Laws
On Behalf of Plaintiffs and the Class

71. Plaintiffs repeat and re-allege the allegations above as if fully set forth herein.

72. Consumer protection statutes exist to ensure that consumers are protected from unfair, deceptive, and unlawful practices.

73. Plaintiffs are "consumers" based upon appliable state consumer protection statutes, and those statutes were enacted to ensure that Defendants did not

engage in unfair, deceptive, and unlawful practices while engaging in trade or commerce.

74. Defendants' conduct offends public policy.

75. As a direct and proximate result of Defendants' unfair trade practices, Plaintiffs and Class Members are entitled to injunctive relief, damages, including actual damages in an amount to be proven at trial or statutory damages, whichever is greater, treble damages of actual damages, and reasonable attorneys' fees, as applicable under various consumer protection statutes.

76. This cause of action will be amended prior to trial based upon discovery and choice of law.

RESERVATION OF RIGHTS TO ASSERT ADDITIONAL CLAIMS FOR RELIEF

77. Plaintiffs have asserted claims in this complaint in order to confer subject matter jurisdiction over Defendants so that this case may be transferred to the District of Montana by the Judicial Panel on Multidistrict Litigation.

78. To the extent this case is transferred back to this Court for trial, Plaintiffs reserve the right to assert additional causes of action or amend their causes of action as applicable and based upon discovery and motion practice in the MDL.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Classes set forth herein, respectfully request the following relief:

a. That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are the proper class representatives; and appoint Plaintiff's counsel as Class Counsel;

b. That the Court grant permanent injunctive relief to prohibit and prevent Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein;

c. That the Court award Plaintiffs and Class Members compensatory,

consequential, general, and/or nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

d. That the Court award punitive or exemplary damages, to the extent permitted by law;

e. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts, omissions, and practices;

f. That Plaintiff be granted the declaratory and injunctive relief to prevent further injuries from manifesting as alleged herein;

g. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

h. That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper; and

i. Any other relief that the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial in the instant action.

Dated: February 3, 2025 Respectfully submitted by:

/s/ Sabita J. Soneji
Sabita J. Soneji, Cal. Bar No. 224262
TYCKO & ZAVAREEI LLP
1970 Broadway, Suite 1070
Oakland, CA 94612
Telephone: (510) 254-6808
ssoneji@tzlegal.com

Jason S. Rathod
MIGLIACCIO & RATHOD LLP
412 H St NE, Suite 302
Washington DC 20002
Tel. 202.470.3520
jrathod@classlawdc.com

John Heenan
HEENAN & COOK
1631 Zimmerman Trail

Billings, MT 59102
Tel. 406.839.9091
john@lawmontana.com

Amy Keller
DICELLO LEVITT LLP
Ten North Dearborn, Sixth Floor
Chicago, Illinois 60602
Tel. 312.214.7900
akeller@dicellolevitt.com

J. Devlan Geddes
GOETZ, GEDDES & GARDNER P.C.
35 N. Grand Ave.
Bozeman, MT 59715
Tel. 406.587.0618
devlan@goetzlawfirm.com

Raphael Graybill
GRAYBILL LAW FIRM, PC
300 4th Street North
Great Falls, MT 59401
Tel. 406.452.8566
raph@graybilllawfirm.com

Counsel for Plaintiffs and the Putative Class